

UNITED STATES DISTRICT COURT  
DISTRICT OF ALASKA

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
TWO ACCOUNT(S) STORED AT  
PREMISES CONTROLLED BY  
GOOGLE LLC FOR INVESTIGATION  
OF VIOLATION OF 18 U.S.C. 2252A



Jan 05 2021

SC No. 1:20-MJ-00084-MMS

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, **Timothy Burman**, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information which is associated with **TWO** account[s] – that is, **liamroody@gmail.com** and **liamrdh.999@gmail.com** – which is stored at premises controlled by **Google LLC** (“PROVIDER”), an electronic communications services provider and/or remote computing services provider which is headquartered at / which accepts service at **1600 Amphitheatre Parkway, Mountain View, California**. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require PROVIDER to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B, using the procedures described in Section III of Attachment B.



Jan 05 2021

2. I am a Special Agent with the Coast Guard Investigative Service. I have been in this position since May, 2019. My duties and responsibilities includes executing and serving federal search warrants and subpoenas, making arrests, and investigation violations of federal law. As a CGIS Special Agent, I have participated in an array of criminal investigations to include sexual assault crimes, drug-related crimes, and crimes involving electronic evidence.

3. I attended and graduated from the Criminal Investigator Training Program (CITP) a three-month academy operated by the Federal Law Enforcement Training Center (FLETC). While attending the academy, I received training on the devices, techniques and practices used by people engaging in the production, storage and distribution of child pornography, as well as the identification, acquisition and preservation of digital evidence. After graduating CITP, I attended CGIS Special Agent Basic Training, a six-week long training course. After this course, I completed field training, which included the investigation of crimes including sexual assault, assault, and felony violations of the Uniform Code of Military Justice.

4. As a CGIS Special Agent, I am responsible for, among other things, conducting investigations that involve, but are not limited to, crimes on the high seas, narcotics smuggling, alien smuggling, and fraudulent use of official documents, and felony violations of the Uniform Code of Military Justice.

5. The facts in this affidavit come from my personal observations, training, experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of **18 U.S.C 2252A** have



Jan 05 2021

been committed by Liam **ROODHOUSE**. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.

### **JURISDICTION**

7. This Court has jurisdiction to issue the requested warrant because it is a “court of competent jurisdiction” as defined by 18 U.S.C. § 2711; 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). As discussed more fully below, acts or omissions in furtherance of the offenses under investigation occurred within Alaska. *See* 18 U.S.C. § 3237.

### **PROBABLE CAUSE**

8. On 04/07/2019, Liam **ROODHOUSE** and victim Rebekah Ambacher began dating. The two met at the Old Town Diner in Valdez, AK. When they began dating, **ROODHOUSE** was 19 years old (born on 04/15/1999), and Ambacher was 16 years old (born on 10/12/2002).

9. On 10/15/2020, during an interview with CGIS Agents, Ambacher claimed she was abused by **ROODHOUSE** during their relationship. She stated **ROODHOUSE** resorted to verbal and physical abuse during their relationship. She claimed **ROODHOUSE** grabbed her by her shoulders and shook her violently when she would “stop responding to him.” **ROODHOUSE** shook her approximately 10 times throughout their relationship.

10. Ambacher stated on 10/02/2020, **ROODHOUSE** observed her exchanging sexually explicit messages with Johnny Chute. **ROODHOUSE** attempted to access Ambacher’s phone to read the messages but could not, due to Ambacher had recently changing the password





Jan 05 2021

on her phone. Ambacher stated later that night, **ROODHOUSE** accessed her Instagram account via his personal cellphone and read the messages she exchanged with Chute. During a subsequent verbal and physical altercation, she stated **ROODHOUSE** climbed on top of her, pinned her down on the bed, and then thrust his clothed penis into her face and mouth five times without her consent, while saying, "This is what you want. You want excitement. I'll give you excitement!"

11. On 11/03/2020, during an interview with CGIS Agents, **ROODHOUSE** waived his rights under Article 31(b), Uniform Code of Military Justice (UCMJ). **ROODHOUSE** admitted to physically assaulting Ambacher three to four times by grabbing her shoulders and shaking her. Additionally, **ROODHOUSE** admitted to accessing Ambacher's Instagram account and reading the messages she exchanged with Chute. **ROODHOUSE** admitted to throwing his own cellphone against the wall, and showed CGIS Agents the damage he had done to his Apple iPhone.

12. During this same interview, **ROODHOUSE** also provided written and verbal consent for CGIS Agents to search his Apple iPhone 12. During the consensual search of **ROODHOUSE**'s Apple iPhone 12, CGIS Agents observed multiple images of Ambacher naked or engaging in sexually explicit actions. These images were saved in the "Photos" application (also known as an "app"), as well as on the social media app "Snapchat" under a contact labeled "Bekah."

13. While CGIS agents were searching **ROODHOUSE**'s Apple iPhone 12, **ROODHOUSE** asked the agents, "anything good in there?" A few minutes later, **ROODHOUSE** told CGIS agents, "There's Google Photos and not so Google Photos... there's definitely 'things' in there... She is cute though, huh? I know what you're seeing." **ROODHOUSE** made these comments when CGIS agents discovered photos of Ambacher nude.



Jan 05 2021

14. The next day, CGIS Agents continued their search of **ROODHOUSE's** Apple iPhone 12. This search revealed that the device was linked to email address **liamroody@gmail.com**, through **ROODHOUSE's** Apple iCloud account. A second **Gmail** address was located on **ROODHOUSE's** Apple iPhone 12, **liamrdh.999@gmail.com**. This email address was associated with **Google Chrome** web browser activity on the following websites <https://api.id.me/>, <https://mobile.facebook.com>, <https://mobile.usaa.com>, <https://pornlive.com> and several others applications.

15. Installed on **ROODHOUSE's** Apple iPhone 12, CGIS Agents also located the following Google apps: **Google Photos, Gmail, and Google Chrome**.

16. Ambacher disclosed to CGIS agents that in May of 2019, when she was 16 years old, she began sending sexually explicit images and videos to **ROODHOUSE** via the social media application "Snapchat." Ambacher stated that after receiving the images on "Snapchat," **ROODHOUSE** would save the images to his camera roll/photos app and the **Google Photos** app on his phone. Ambacher claimed these images and videos showed her fully nude, and often engaged in various sexually explicit acts such as masturbation.

17. Ambacher claimed that she continued to send sexually explicit images and videos to **ROODHOUSE** until they broke up on or about 10/05/2020, shortly before her 18<sup>th</sup> birthday. She estimated that she had shared over 100 sexually explicit images and videos with **ROODHOUSE**. Ambacher admitted that when she took the sexually explicit images and videos, and sent them to **ROODHOUSE**, she was under the age of 18.

18. Ambacher told CGIS Agents **ROODHOUSE** currently owned an Apple iPhone 12, but he had previously owned an LG brand cellphone.



Jan 05 2021

19. Based on my training and experience, LG cellphones operate on the Android operating system that is commercially sponsored by Google LLC. Additionally, Android devices, including LG branded devices, ship with the Google Mobile Services application suite. This includes **Google Search, Google Chrome, YouTube, Google Play Store, Gmail, Google Photos, and Google Drive** among others.

20. On 10/21/2020 during an interview with CGIS Agents, Caitlin Way, Owner of Fisheye Coffee in Sitka, AK, Ambacher's prior employer, provided a copy of an email sent by **ROODHOUSE**. The email subject line was titled "disappointed," and was received from "Liam Roodhouse" at the email address **liamroody@gmail.com**.

21. On 11/25/2020, CGIS Agents served PROVIDER with a preservation letter under 18 U.S.C. § 2703(f) related to **liamroody@gmail.com** and **liamrdh.999@gmail.com**.

#### **BACKGROUND CONCERNING PROVIDER'S ACCOUNTS**

22. PROVIDER is the provider of the internet-based account(s) identified by **liamroody@gmail.com** and **liamrdh.999@gmail.com**.

23. PROVIDER provides its subscribers internet-based accounts that allow them to send, receive, and store e-mails online. PROVIDER accounts are typically identified by a single username, which serves as the subscriber's default e-mail address, but which can also function as a subscriber's username for other PROVIDER services, such as instant messages and remote photo or file storage.

24. Based on my training and experience, I know that PROVIDER allows subscribers to obtain accounts by registering on PROVIDER's website. During the registration process, PROVIDER asks subscribers to create a username and password, and to provide basic personal information such as a name, an alternate e-mail address for backup purposes, a phone number, and





in some cases a means of payment. PROVIDER typically does not verify subscriber names. However, PROVIDER does verify the e-mail address or phone number provided.

25. Once a subscriber has registered an account, PROVIDER provides e-mail services that typically include folders such as an “inbox” and a “sent mail” folder, as well as electronic address books or contact lists, and all of those folders are linked to the subscriber’s username. PROVIDER subscribers can also use that same username or account in connection with other services provided by PROVIDER; The services may include: electronic communication services such as Google Voice (voice calls, voicemail, and SMS text messaging, Hangouts (instant messaging and video chats), Google Photos (photo sharing), YouTube (video sharing); web browsing and search tools such as Google Search (internet searches), Web History (bookmarks and recorded browsing history), and Google Chrome (web browser), online productivity tools such as Google Calendar, Google Contacts, Google Docs (word processing, Google Drive (cloud storage); online tracking and advertising tools such as Google Analytics (track and reporting on website traffic) and Google AdWords (user targeting based on search queries).

26. In general, user-generated content (such as e-mail) that is written using, stored on, sent from, or sent to a PROVIDER account can be permanently stored in connection with that account, unless the subscriber deletes the material. For example, if the subscriber does not delete an e-mail, the e-mail can remain on PROVIDER’s servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to exist on PROVIDER’s servers for a certain period of time.

27. Thus, a subscriber’s PROVIDER account can be used not only for e-mail but also for other types of electronic communication, including instant messaging and photo and video sharing; voice calls, video chats, SMS text messaging; social networking. Depending on user settings, user-generated content derived from many of these services is normally stored on



PROVIDER's servers until deleted by the subscriber. Similar to e-mails, such user-generated content can remain on PROVIDER's servers indefinitely if not deleted by the subscriber, and even after being deleted, it may continue to be available on PROVIDER's servers for a certain period of time. Furthermore, a PROVIDER subscriber can store contacts, calendar data, images, videos, notes, documents, bookmarks, web searches, browsing history, and various other types of information on PROVIDER's servers. Based on my training and experience, I know that evidence of who controlled, used, and/or created a PROVIDER account may be found within such computer files and other information created or stored by the PROVIDER subscriber. Based on my training and experience, I know that the types of data discussed above can include records and communications that constitute evidence of criminal activity.

28. Based on my training and experience, I know that providers such as PROVIDER also collect and maintain information about their subscribers, including information about their use of PROVIDER services. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. Providers such as PROVIDER also commonly have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with other logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which devices were used to access the relevant account. Also, providers such as PROVIDER typically collect and maintain location data related to subscriber's use of PROVIDER services, including data derived from IP addresses and/or Global Positioning System ("GPS") data.





Jan 05 2021

29. Based on my training and experience, I know that providers such as PROVIDER also collect information relating to the devices used to access a subscriber's account – such as laptop or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or “hardware,” some identifiers are assigned by a telephone carrier concerning a particular user account for cellular data or voice services, and some identifiers are actually assigned by PROVIDER in order to track what devices are using PROVIDER's accounts and services. Examples of these identifiers include unique application number, hardware model, operating system version, Global Unique Identifier (“GUID”), device serial number, mobile network information, telephone number, Media Access Control (“MAC”) address, and International Mobile Equipment Identity (“IMEI”). Based on my training and experience, I know that such identifiers may constitute evidence of the crimes under investigation because they can be used (a) to find other PROVIDER accounts created or accessed by the same device and likely belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during course of the investigation was used to access the PROVIDER account.

30. Based on my training and experience, I know that providers such as PROVIDER use cookies and similar technologies to track users visiting PROVIDER's webpages and using its products and services. Basically, a “cookie” is a small file containing a string of characters that a website attempts to place onto a user's computer. When that computer visits again, the website will recognize the cookie and thereby identify the same user who visited before. This sort of technology can be used to track users across multiple websites and online services belonging to PROVIDER. More sophisticated cookie technology can be used to identify users across devices



Jan 05 2021

and web browsers. From training and experience, I know that cookies and similar technology used by providers such as PROVIDER may constitute evidence of the criminal activity under investigation. By linking various accounts, devices, and online activity to the same user or users, cookies and linked information can help identify who was using a PROVIDER account and determine the scope of criminal activity.

31. Based on my training and experience, I know that PROVIDER maintains records that can link different PROVIDER accounts to one another, by virtue of common identifiers, such as common e-mail addresses, common telephone numbers, common device identifiers, common computer cookies, and common names or addresses, that can show a single person, or single group of persons, used multiple PROVIDER accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular PROVIDER account.

32. Based on my training and experience, I know that subscribers can communicate directly with PROVIDER about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as PROVIDER typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

33. In summary, based on my training and experience in this context, I believe that the computers of PROVIDER are likely to contain user-generated content such as stored electronic communications (including retrieved and un-retrieved e-mail for PROVIDER subscribers), as well



Jan 05 2021

as PROVIDER-generated information about its subscribers and their use of PROVIDER services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide PROVIDER with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

34. As explained above, information stored in connection with a PROVIDER account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of the offense, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with a PROVIDER account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by PROVIDER can show how and when the account was accessed or used. For example, providers such as PROVIDER typically log the IP addresses from which users access the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the PROVIDER account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculcate or exculpate the person who controlled, used, and/or created the account. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a





Jan 05 2021

particular time (*e.g.*, location information integrated into an image or video sent via e-mail). Finally, stored electronic data may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information in the PROVIDER account may indicate its user's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

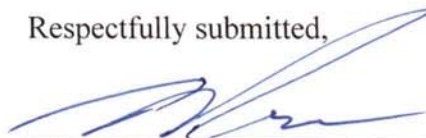
**REQUEST TO SUBMIT WARRANT BY TELEPHONE  
OR OTHER RELIABLE ELECTRONIC MEANS**

35. I respectfully request, pursuant to Rules 4.1 and 41(d)(3) of the Federal Rules of Criminal Procedure, permission to communicate information to the Court by telephone in connection with this Application for a Search Warrant. If I were required to appear before the Court in person, it would be a cost to the United States both in travel costs and time diverted from the substantive investigation. I submit that Special Assistant U.S. Attorney Steven Caouette, an attorney for the United States, is capable of identifying my voice and telephone number for the Court.

**CONCLUSION**

36. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on PROVIDER, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,



Timothy R. Burman  
Special Agent  
Coast Guard Investigative Service

Subscribed and sworn to pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on 01/04/2021.

  
UNITED STATES DISTRICT JUDGE